**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION – ANN ARBOR**

IN RE DOCUMENT SUBPOENA OF NON-PARTY UNIVERSITY OF MICHIGAN TRANSPORTATION RESEARCH INSTITUTE FCA US LLC c/o Thompson Coburn LLP One US Bank Plaza St. Louis, MO 63101, Movant.	CASE NO. _______
BRIAN FLYNN, GEORGE and KELLY BROWN, and MICHAEL KEITH, on behalf of Themselves and all others similarly situated, Plaintiffs, v. FCA US LLC f/k/a CHRYSLER GROUP LLC And HARMAN INTERNATIONAL INDUSTRIES, INCORPORATED, Defendants.	United States District Court, Southern District of Illinois, C.A. No. 3:15-cv-00855

**FCA US LLC'S MOTION TO QUASH
THIRD-PARTY SUBPOENA SERVED ON UNIVERSITY OF MICHIGAN
TRANSPORTATION RESEARCH INSTITUTE**

Movant FCA US LLC, Defendant in the underlying action, moves this Court for an order, pursuant to Rule 45(d)(3) of the Federal Rules of Civil Procedure, quashing the subpoena directed to non-party University of Michigan Transportation Research Institute, a business provider to FCA US that possesses confidential cybersecurity information belong to FCA US. In support of its Motion, FCA US states as follows:

1. Plaintiffs in an Underlying Action asserting product defect claims have subpoenaed non-party University of Michigan Transportation Research Institute ("UMTRI") for documents.

2. UMTRI is a research institution that Movant FCA US retained to study intrusion detection systems for its vehicles.

3. FCA US provided its confidential information to UMTRI as part of the engagement, which the parties contractually agreed would remain confidential.

4. The Cybersecurity Information Act of 2015 requires that such information remain confidential in accordance with the parties' agreement. *See* 6 U.S.C. § 1503(c)(2).

5. Moreover, even if The Cybersecurity Information Act of 2015 did not require nondisclosure, the Court should quash subpoena in its discretion under Fed. R. Civ. P. 45(d)(3)(B) to protect FCA US's confidential information.

6. Besides being confidential, the information sought by the subpoena is also irrelevant to the claims and defenses in the Underlying Action, and the subpoena should be quashed on this additional ground. *See* Fed. R. Civ. P. 26(b)(1).

7. This Motion is made following a conference with counsel for Plaintiffs in the underlying action, *Flynn v. FCA US LLC*, No. 3:15-cv-00855 (S.D. Ill.), pursuant to L.R. 7-1(a), which took place on April 3, 2017, in which counsel for FCA US explained the nature of this Motion and its legal basis. FCA US did not obtain concurrence in the relief sought. Counsel for FCA US and Plaintiffs' counsel were unable to resolve their differences as they relate to the subpoena at issue. Counsel for FCA US understands that this motion to quash will be opposed.

8. FCA US additionally conferred with counsel for non-party University of Michigan Transportation Research Institute regarding the third-party subpoena on March 23, 2017 and April 3, 2017. FCA US explained the nature of its motion, and its legal basis. University of Michigan Transportation Research Institute does not oppose FCA US's motion.

9. In further support of its Motion, FCA US adopts and incorporates by reference its accompanying Brief.

FOR RELIEF, Defendant FCA US LLC respectfully requests that this Court quash the third-party subpoena served on University of Michigan Transportation Research Institute, and grant FCA US all other appropriate relief.

Respectfully submitted,

s/ Larry J. Saylor
MILLER, CANFIELD, PADDOCK AND STONE, P.L.C.
150 West Jefferson, Suite 2500
Detroit, MI 48226
(313) 963-6420
saylor@millercanfield.com
(P28165)

THOMPSON COBURN LLP
Kathy A. Wisniewski
Stephen A. D'Aunoy
Sharon B. Rosenberg
One US Bank Plaza
St. Louis, MO 63101
(314) 552-6000
kwisniewski@thompsoncoburn.com
sdaunoy@thompsoncoburn.com
srosenberg@thompsoncoburn.com

Attorneys for Movant FCA US LLC

Dated: April 4, 2017

LOCAL RULE CERTIFICATION

I, Larry J. Saylor, certify that this document complies with Local Rule 5.1(a), including: double-spaced (except for quoted materials and footnotes); at least one-inch margins on the top, sides and bottom; consecutive page numbering; and type size of all text and footnotes that is no smaller than 10-1/2 characters per inch (for non-proportional fonts) or 14 point (for proportional fonts). I also certify that it is the appropriate length. Local Rule 7.1(d)(3).

s/ *Larry J. Saylor*

CERTIFICATE OF SERVICE

I, Larry J. Saylor, counsel for movant FCA US LLC and a member of the Bar of this Court, certify that on April 4, 2017, I caused a copy of FCA US LLC's Brief in Support of Its Motion to Quash Third-Party Subpoena Served on University of Michigan Transportation Research Institute to be served by overnight mail on the following:

Stephen R. Wiggington
Christopher D. Baucom
Lucas T. Pendry
Armstrong Teasdale LLP
7700 Forsyth Blvd., Suite 1800
St. Louis, MO 63105-1810

IJay Palansky
Emily Buckley
Armstrong Teasdale LLP
4643 S. Ulster St., St. 800
Denver, CO 80237

Christopher F. Cueto
Lloyd M. Cueto
Michael J. Gras
Law Office of Christopher Cueto
7110 West Main Street
Belleville, IL 62223

Counsel for Plaintiffs Brian Flynn, George and Kelly Brown, and Michael Keith

Andrew Blair Fromm
John R. Trentacosta
Vanessa L. Miller
Foley & Lardner LLP
500 Woodward Ave., Suite 2700
Detroit, MI 48226-3489

Elizabeth Mazzocco
William J. McKenna, Jr.
Foley & Lardner LLP
321 North Clark Street, Suite 2800
Chicago, IL 60654

Michael D. Leffel
Foley & Lardner LLP
150 East Gilman Street
P.O Box 1497
Madison, WI 53703-1481

Counsel for Defendant Harman International Industries, Inc.

I further certify that all parties required to be served have been served.

s/ *Larry J. Saylor*

28901391.1\155704-00006

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION – ANN ARBOR

IN RE DOCUMENT SUBPOENA OF NON-PARTY UNIVERSITY OF MICHIGAN TRANSPORTATION RESEARCH INSTITUTE FCA US LLC c/o Thompson Coburn LLP One US Bank Plaza St. Louis, MO 63101, Movant.	CASE NO. _______
BRIAN FLYNN, GEORGE and KELLY BROWN, and MICHAEL KEITH, on behalf of Themselves and all others similarly situated, Plaintiffs, v. FCA US LLC f/k/a CHRYSLER GROUP LLC And HARMAN INTERNATIONAL INDUSTRIES, INCORPORATED, Defendants.	United States District Court, Southern District of Illinois, C.A. No. 3:15-cv-00855

FCA US LLC'S BRIEF IN SUPPORT OF ITS MOTION TO QUASH THIRD-PARTY SUBPOENA SERVED ON UNIVERSITY OF MICHIGAN TRANSPORTATION RESEARCH INSTITUTE

ISSUES PRESENTED

1. Whether the subpoena served on the University of Michigan Transportation Research Institute ("UMTRI") seeks confidential cybersecurity information which FCA US and UMTRI have lawfully agreed not to disclose to third parties, and the disclosure of which is thereby barred by The Cybersecurity Act of 2015, 6 U.S.C. § 1501, *et seq.*?

2. Whether the information sought by the subpoena served on UMTRI is relevant to the claims or defenses in the underlying product defect action, where it does not concern any of the defects alleged?

CONTROLLING AUTHORITY

The Cybersecurity Act of 2015, 6 U.S.C. § 1501, *et seq.*

Fed. R. Civ. P. 26(b)(1)

Fed. R. Civ. P. 45(d)(3)(B)

I. INTRODUCTION

Pursuant to Rule 45(d)(3) of the Federal Rules of Civil Procedure, FCA US LLC has moved to quash the subpoena directing non-party, the University of Michigan Transportation Research Institute ("UMTRI") to produce documents in a civil action (the "Subpoena"). The Subpoena was issued by the plaintiffs in the underlying action which is pending in the United States District Court for the Southern District of Illinois (the "Underlying Action"). The Subpoena directs UMTRI to produce several broad categories of documents, all related to cybersecurity work performed by UMTRI, pursuant to contract, for FCA US. Each category contemplates the production of documents which contain FCA US's confidential information.

FCA US moves to quash the Subpoena because UMTRI's compliance would result in it disclosing FCA US's confidential and proprietary information, and the information lacks relevance to the Underlying Action.

II. BACKGROUND

A. The Underlying Action.

Plaintiffs filed the Underlying Action against FCA US and Harman International Industries, Incorporated on August 4, 2015, approximately two weeks after two highly and uniquely skilled cybersecurity researching experts demonstrated that they had engineered a way to remotely control certain functions on a Jeep Cherokee vehicle. *See* Class Action Comp., *Flynn v. FCA US LLC*, ECF #1 (attached as **Appendix A**) and Am. Class Action Comp., *Flynn v. FCA US LLC*, ECF #49 (attached as **Appendix B**). This controlled experiment is the only known instance of an FCA US vehicle ever being remotely "hacked." Following the experiment, FCA US issued a recall remedy under the supervision of the National Highway Traffic Safety Administration ("NHTSA"), to correct the vulnerability which allowed the researchers to conduct the hack. Since the recall, there have been no known instances of remote hacking of any FCA US vehicle. *See generally* FBI/NHTSA Joint PSA (Mar. 17, 2016) (attached as **Appendix C**).

In their lawsuit, Plaintiffs allege, *inter alia*, that certain FCA US vehicles suffer from design defects that make them vulnerable to remote hacking, even after the recall remedy, and that FCA US knew about the potential for hacks but failed to disclose it. App. B ¶¶ 1-2.[1] Plaintiffs allege three specific defects: (1) cybercriminals may remotely access a vehicle; (2) once a vehicle is accessed, cybercriminals may remotely take control of its functions; and (3) the vehicles are not able to receive software security patches "over the air." *Id.* at ¶¶ 18-20.

---

[1]The Southern District of Illinois has dismissed certain of the claims brought by some Plaintiffs. *See* Mem. & Order, *Flynn v. FCA US LLC* (Sept. 23, 2016), ECF #115 (attached as **Appendix K**). A motion to dismiss claims brought by other Plaintiffs is pending.

B. Discovery in the Underlying Action.

Plaintiffs have served discovery in the Underlying Action, including five sets of document requests and five sets of interrogatories on FCA US, and subpoenas on ***more than fifteen*** non-parties. *See*, *e.g.*, Subpoena to Non-Party Auto-ISAC (attached as **Appendix D**).

Only one non-party moved to quash a subpoena served by Plaintiffs, *i.e.*, Auto-ISAC, a non-profit organization in which FCA US and other auto manufacturers confidentially share information regarding cybersecurity threats. The District Court presiding over the Underlying Action quashed the subpoena, finding that Plaintiffs' quest for documents constituted a "fishing expedition." *See* Mem. & Order, *Flynn v. FCA US LLC* (Nov. 30, 2016), ECF #30 (attached as **Appendix E**), pp. 4-5.

C. UMTRI and FCA US's Engagement of UMTRI

UMTRI is a research institution "dedicated to achieving safe and sustainable transportation for a global society." *See* http://www.umtri.umich.edu/who-we-are (attached as **Appendix F**). "As an institute UMTRI combines the flexibility and ability ***to keep proprietary information confidential*** with the creativity of a university environment by being able to deploy experienced full-time engineers and/or engineering students as it fits best in terms of project sensitivity and objective." *See* http://www.umtri.umich.edu/our-focus/cybersecurity (emphasis added) (attached as **Appendix G**).

In or about March 2015, pursuant to a written contract, FCA US retained UMTRI to provide cybersecurity expertise in the field of CAN-bus message intrusion detection systems. *See* FCA US/ UMTRI Agreement (attached as **Appendix H**) ("FCA US/UMTRI Agreement"). An intrusion detection system (IDS) looks for anomalies with the equipment seeking to communicate with the CAN-bus, which is a vehicle's communication hub. An IDS can red-flag an attack from a third-party spoofing commands to the vehicle. ***The FCA US/UMTRI Agreement contains a provision ensuring the confidentiality of FCA US's information***. *See id.* at § 13. The FCA US/UMTRI Agreement requires UMTRI to "cooperate with FCA US's reasonable attempts to limit such disclosure in a manner which attempts to maintain the confidentiality of the subject FCA US Proprietary Information to the fullest extent permitted by law." *Id.*

D. The Subpoena.

On January 25, 2017, Plaintiffs served a subpoena on UMTRI commanding the production of documents in Ann Arbor, Michigan on February 21, 2017.[2] *See* the Subpoena (attached as **Appendix I**). In the UMTRI Subpoena, Plaintiffs seek the following documents:

---

[2]This Court, therefore, has jurisdiction over this Motion to Quash. *See* Fed.R.Civ.P. 45(d)(3)(B).

> 1. All documents (including communications, such as emails) relating to any cybersecurity-related work You performed on or regarding FCA's vehicles or Harman's infotainment systems during the period January 1, 2012 to present. This should include, but should not be limited to, cybersecurity testing; diagnosis or identification of cybersecurity vulnerabilities, exploits, or threats; and analysis or consideration of any remedial, response, or mitigation actions to address cybersecurity vulnerabilities, exploits, threats, or hacks.
>
> 2. All documents and communications regarding, concerning, or referring to UMTRI's "Intrusion Detection System Analysis" project conducted for FCA during the period January 1, 2012 to present.
>
> 3. All document regarding, concerning, constituting, or referring to UMTRI's suggestions, changes, or recommendations to the internal architecture of FCA's vehicles, including all drafts thereof, created during the period January 1, 2012 to present.

Id. Plaintiffs have ***not*** requested this same information from FCA US in the Underlying Action.

UMTRI was served with the subpoena on or around January 25, 2017. *Id.* UMTRI has not yet objected to the Subpoena, but reached an agreement with Plaintiffs under which it was allowed time to discuss with FCA US, its client, FCA US's position on the disclosure of its confidential information.

After receiving a letter from UMTRI about the possibility that responding to the Subpoena could result in the disclosure of FCA US's confidential information, FCA US immediately attempted to make contact with UMTRI, but the parties were not able to speak until March 15, 2017. Declaration of S. Rosenberg (attached as **Appendix J**), ¶¶ 3-5. At the time of the initial contact, UMTRI could not verify what confidential information would be responsive to the Subpoena or the volume of responsive materials, but indicated it was in the process of compiling such information. *Id.* at ¶ 6. Counsel for FCA US advised UMTRI that it wanted the confidentiality provisions of the FCA US/UMTRI Agreement enforced to the fullest extent. *Id.* at ¶ 7.

On March 23, 2017, UMTRI advised FCA US, for the first time, that the documents responsive to the Subpoena it held would in fact reveal FCA US's confidential information. *Id.* at ¶ 8. Specifically, UMTRI informed FCA US that its materials included files with proprietary information about the CAN-bus system, including but not limited to non-public information such as .dbc files, which is a format used to hold all the information on a CAN-bus system. *Id.* at ¶ 9. FCA US reiterated its position that UMTRI must abide by the FCA US/ UMTRI Agreement and protect all such documents under its confidentiality provisions. *Id.* at ¶ 10.

Subsequently, on March 27, 2017, UMTRI informed FCA US that: (1) it could not identify specifically which responsive documents contained trade secrets or other confidential information; (2) given the high volume of documents responsive to the Subpoena, it was unable or unwilling to review the documents in order to identify specifically which documents contained trade secrets or other confidential information; and (3) based on a lack of organization of the collected materials and the volume of documents, it would be equally burdensome or impracticable for FCA US to review the documents in advance of production to determine which are confidential.[3] *Id.* at ¶ 11. UMTRI also informed FCA US that it would not move to quash the Subpoena. *Id.* at ¶ 12.

III. ARGUMENT

A. The Subpoena Should be Quashed Because Federal Law Requires the Enforcement of FCA US's Confidentiality Agreement with UMTRI.

FCA US has standing to move to quash the Subpoena because it is an affected party. Rule 45 permits a court to quash a subpoena "[t]o protect a person subject to ***or affected by*** a subpoena" if the subpoena requires "disclosing a trade secret or other confidential research, development, or commercial information." Fed.R.Civ. P. 45(d)(3)(B) (emphasis added); *see also Ajuba Int'l, LLC v. Saharia*, No. 11-cv-12936, 2014 WL 4793846, *2 (E.D. Mich. Sept. 25, 2016) (applying rule to allow party to move to quash non-party subpoena where responsive materials contained his confidential information); *Woods v. Fresenius Med. Care Grp. of N. Am.*, No. 1:06-cv-1804, 2008 WL 151836, *1 (S.D. Ind. Jan. 16, 2008) (same) (citing *United States v. Raineri*, 670 F.2d 702, 712 (7th Cir. 1982)).

---

[3]While UMTRI has not asserted its own burden as grounds to quash the Subpoena, UMTRI has avoided substantial burden of reviewing the documents only by refusing to provide FCA US with specific information regarding which responsive materials contain FCA US's proprietary and confidential information, thereby shifting the risk, the burden, and the prejudice to FCA US.

Here, FCA US is affected by the Subpoena not only because compliance would require disclosure of ***its*** confidential information, and because it has contractual rights of confidentiality at stake that UMTRI has refused to enforce, but also because the cybersecurity implications here entitle it to special protections and require nondisclosure.

Respect for the confidentiality of trade secrets and other proprietary information, already reflected in Rule 45(d)(3), is at its height in the cybersecurity realm, and such information is afforded special status by federal law. As part of The Cybersecurity Act of 2015, federal law mandates that confidential cybersecurity information ***remain confidential*** in accordance with confidentiality agreements between private parties:

> A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity … shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity.

6 U.S.C. § 1503(c)(2).

"Cyber threat indicator" and "defensive measure" are both defined broadly under the Act, encompassing among other things any information that is necessary to describe or identify: "a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability"; "malicious cyber command and control"; or "any other attribute of a cybersecurity threat"; and "an action … that detects … a known or suspected cybersecurity threat or security vulnerability." 6 U.S.C. §§ 1501(6), (7). Here, of course, the information received by UMTRI specifically relates to intrusion detection systems, *i.e.*, detection of unlawful cyber-intrusions and malicious cyber command of the CAN-bus system. The information called for by the Subpoena therefore falls squarely under the Act's protections.[4]

---

[4]Because a federal statute governs here and requires nondisclosure, FCA US does not provide a lengthy recital of generally applicable principles of confidentiality under Rule 45(d). These standards are easily met, however. *See Spartanburg Reg'l Healthcare Sys. v. Hillenbrand Indus.*, No. 1:05-MC-107, 2005 WL 2045818, *3 (W.D. Mich. Aug. 24, 2005), *aff'd*, 2005 WL 2571943 (W.D. Mich. Oct. 12, 2005) (evaluating confidentiality of information under Rule 45, considering issues of sensitivity of information and harm from disclosure). FCA US carefully guards cybersecurity information, as reflected by the Confidentiality Agreement itself, and its release could create cybersecurity risks that don't exist now, with societal costs to consumers and economic costs to FCA US—the very harm that The Cybersecurity Act was designed to prevent. Thus, even if for some reason the Court found that the Act did not apply and bar disclosure, the Court should nevertheless exercise its discretion under Rule 45(d) to quash the Subpoena.

This statute is mandatory and unambiguous, and thus the Court need not resort to public policy considerations. But, in any event, the public policy on which the statute is based is sound. The Cybersecurity Act was designed "to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats." S.2588, 113th Congress, 2d Session (June 11, 2014). Although FCA US dedicates significant resources to cybersecurity, it is not a cybersecurity company. To serve the societal interest, it is thus necessary for FCA US (like virtually every other large company on the planet) to share confidential information about cybersecurity threats, vulnerabilities, and research with third-party experts. The Cybersecurity Act recognizes this free-exchange of information between technology and manufacturing companies as critical to cybersecurity in the 21st Century.

If cybersecurity vendors like UMTRI were permitted to disclose confidential cybersecurity information belonging to third parties (to whom it owes contractual confidentiality obligations, no less), then manufacturers seeking to maximize the security of their products would be reluctant to seek necessary outside expertise.[5]

---

[5]A protective order is in place in the Underlying Action (*Flynn v. FCA US LLC*, ECF #148), but its existence does not negate confidentiality concerns, as it allows information to be shared with Plaintiffs' experts, *i.e.* the very cybersecurity experts from whom this information is carefully guarded. And, in any case, The

The need to prevent this chilling effect, codified in The Cybersecurity Act, only reinforces the importance of quashing the Subpoena here. *Cf. In re Fosamax Prods. Liab. Litig.*, 2009 WL 2395899 (S.D.N.Y. Aug. 4, 2009) (quashing subpoena to depose a researcher in part because compelling testimony would "risk[] chilling participation in beneficial public research," and "the resulting social impact would be … serious"). Under the provisions of The Cybersecurity Act, and the policy it codifies as law, the Subpoena must be quashed.

B. The Subpoena Should be Quashed Because the Plaintiffs Seek Irrelevant Information.

Even if the requested information were not subject to federal requirements that confidentiality be maintained (and it is), this Court should still squash the Subpoena because it seeks documents that are irrelevant to the claims in the Underlying Action. A non-subpoenaed party that is affected by the subpoena may challenge the relevance of the information sought. *See, e.g., Kimberly-Clark Corp. v. Baxter Healthcare Corp.*, No. 93 C 6886, 1993 WL 524376, at *2 (N.D. Ill. Dec. 13, 1993) ("K-C therefore does have standing to object to its opponents' invoking this court's powers to try to obtain from a third party settlement documents in

---

Cybersecurity Act does not allow an exception for when a protective order is in place, presumably because a protective order does not eliminate the Act's paramount concerns about a chilling effect. *See* 6 U.S.C. § 1503(c)(2).

which K-C has an interest and which it contends are irrelevant to and should not be produced or used in the underlying actions"); *Woods*, 2008 WL 151836, at *2 (granting party's motion to quash subpoena issued to non-party on relevance grounds).

The Federal Rules of Civil Procedure provide that parties may only "obtain discovery regarding any nonprivileged matter that is ***relevant*** to any party's claim or defense," provided, of course, that it is also "proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1) (emphasis added). "[I]f the information is irrelevant," then discovery directed towards that information "is outside the scope of Rule 26(b)." *Freytag v. Ford Motor Co.*, No. 15-CV-13569, 2016 WL 2957934, *2 (E.D. Mich. May 23, 2016).

In quashing a non-party subpoena issued by Plaintiffs seeking cybersecurity information, the District Court presiding over the Underlying Action offered an analysis of relevance that is equally applicable here. Referring to a subpoena Plaintiffs served on Auto-ISAC, that court (the one with the most intimate knowledge about this case), indicated that while "Plaintiffs' theme in the case" may extend to the "knowledge of and responses to [all] perceived or known [cybersecurity] threats," their claims do not extend nearly so far. App. E, at 5.

Plaintiffs put three specific alleged defects at issue. App. B ¶¶ 18-20. These defects do not implicate a claim that FCA US can or cannot detect an intrusion into a CAN-bus system. Yet, the documents sought in the Subpoena are directed to this. The Subpoena should be quashed because Plaintiffs are "not entitled to amass a collection of documents in hopes of finding something useful" even though not related to the defects they allege. *Woods*, 2008 WL 151836, at *2.

It is noteworthy that the Subpoena seeks documents that could only be used in an attempt to learn how to hack a vehicle that is not known to be currently hackable in any way. Plaintiffs' theory of liability in the Underlying Action is that their vehicles have diminished in value because a random cybercriminal off the street will be able to hack them; their theory is ***not*** that someone will steal FCA US confidential documents provided to a third-party cybersecurity expert and use them to discover an as-yet unknown way to hack a vehicle. In other words, if Plaintiffs cannot prove that their vehicles can be remotely hacked without access to confidential information that others in the general public do not have access to, then they lose, because as of now (since the recall fix) no one has been able to remotely hack the vehicles at issue, not even highly and uniquely skilled cybersecurity geniuses in highly controlled experiments. Plaintiffs should not be given the secret map leading to the undiscoverable because this does nothing to show that "anyone can find it." By issuing the Subpoena, effectively what

Plaintiffs seem to believe is that with access to enough confidential information, the vehicles can be hacked. Even if this ultimately proved true, it would be irrelevant to Plaintiff's theory that the vehicles are so susceptible to hacking today they have a diminished value.

Relevance must be determined by reference to the specific claims and defenses in the lawsuit. *See Shathaia v. Travelers Cas. Ins. Co. of Am.*, No. 12-CV-13657, 2014 WL 197734, *4 (E.D. Mich. Jan. 16, 2014). The claims at issue do not concern what might happen if someone got ahold of FCA US confidential documents. Nor do they concern what FCA US did or did not do generally with respect to cybersecurity measures. *See* App. K at 24. The documents sought by the Subpoena do not touch on the relevant issues left in the case, *i.e.*, the existence of a purported defect unrelated to intrusion detection, the effectiveness of the recall remedy, and FCA US's pre-existing knowledge in order to support a concealment claim. Accordingly, the Subpoena should be quashed.

IV. CONCLUSION

For the foregoing reasons, FCA US respectfully requests that the Court quash the document subpoena served by Plaintiffs in the Underlying Action on non-party University of Michigan Transportation Research Institute.

Respectfully submitted,

s/ Larry J. Saylor

MILLER, CANFIELD, PADDOCK AND STONE, P.L.C.
150 West Jefferson, Suite 2500
Detroit, MI 48226
(313) 963-6420
saylor@millercanfield.com
(P28165)

THOMPSON COBURN LLP
Kathy A. Wisniewski
Stephen A. D'Aunoy
Sharon B. Rosenberg
One US Bank Plaza
St. Louis, MO 63101
(314) 552-6000
kwisniewski@thompsoncoburn.com
sdaunoy@thompsoncoburn.com
srosenberg@thompsoncoburn.com

Attorneys for Movant FCA US LLC

Dated: April 4, 2017

LOCAL RULE CERTIFICATION

I, Larry J. Saylor, certify that this document complies with Local Rule 5.1(a), including: double-spaced (except for quoted materials and footnotes); at least one-inch margins on the top, sides and bottom; consecutive page numbering; and type size of all text and footnotes that is no smaller than 10-1/2 characters per inch (for non-proportional fonts) or 14 point (for proportional fonts). I also certify that it is the appropriate length. Local Rule 7.1(d)(3).

s/ *Larry J. Saylor*

CERTIFICATE OF SERVICE

I, Larry J. Saylor, counsel for movant FCA US LLC and a member of the Bar of this Court, certify that on April 4, 2017, I caused a copy of FCA US LLC's Brief in Support of Its Motion to Quash Third-Party Subpoena Served on University of Michigan Transportation Research Institute to be served by overnight mail on the following:

Stephen R. Wiggington
Christopher D. Baucom
Lucas T. Pendry
Armstrong Teasdale LLP
7700 Forsyth Blvd., Suite 1800
St. Louis, MO 63105-1810

IJay Palansky
Emily Buckley
Armstrong Teasdale LLP
4643 S. Ulster St., St. 800
Denver, CO 80237

Christopher F. Cueto
Lloyd M. Cueto
Michael J. Gras
Law Office of Christopher Cueto
7110 West Main Street
Belleville, IL 62223

Counsel for Plaintiffs Brian Flynn, George and Kelly Brown, and Michael Keith

Andrew Blair Fromm
John R. Trentacosta
Vanessa L. Miller
Foley & Lardner LLP
500 Woodward Ave., Suite 2700
Detroit, MI 48226-3489

Elizabeth Mazzocco
William J. McKenna, Jr.
Foley & Lardner LLP
321 North Clark Street, Suite 2800
Chicago, IL 60654

Michael D. Leffel
Foley & Lardner LLP
150 East Gilman Street
P.O Box 1497
Madison, WI 53703-1481

Counsel for Defendant Harman International Industries, Inc.

I further certify that all parties required to be served have been served.

s/ *Larry J. Saylor*

28901430.1\155704-00006